

移动互联网安全框架

Security Framework of Mobile Internet

中图分类号:TN929.5; TP393.4 文献标识码:A 文章编号:1009-6868 (2009) 04-0028-04

摘要: 文章认为应当采用物理与信息安全分层,依据移动互联网网络结构,构建移动互联网安全架构。按照网络特征,移动互联网可以分终端、网络以及业务系统3个部分;网络与信息安全分设备/环境安全、业务应用安全、信息自身安全以及信息内容安全4个层面。移动互联网安全应将终端、网络以及业务系统分别在设备/环境、业务应用、信息自身以及信息内容安全层面加以研究。

关键词: 移动互联网;网络与信息安全;安全框架

Abstract: The article describes the layered model of network and information security, and gets the security framework of mobile Internet according to the structure of mobile Internet. The mobile Internet has three parts, i.e. terminal, network and service system, and the network and information security; and it can be studied in 4 layers: equipment/environment security layer, service and application security layer, information security layer and information content security layer.

Key words: mobile Internet; network and information security; security framework

魏亮/WEI Liang

(工业和信息化部电信研究院,北京 100045)

(China Academy of Telecommunication

Research of MIIT, Beijing 100045, China)

随着信息化水平的提高,互联网逐渐深入到使用者的日常生活,人们对互联网使用的需求也随之水涨船高。除了在家和在办公室接入互联网外,出现了随时随地,在移动过程中,在野外,在地铁等交通工具中接入互联网的需求。与此同时,无线技术的飞速发展也为此提供了相应的技术支撑,除了无线局域网(如Wi-Fi)技术外,还有WCDMA、CDMA2000 EV-DO、TD-SCDMA、WiMAX等3G移动通信技术。据中国互联网信息中心(CNNIC)统计,截至2008年底,中国移动互联网的用户数达到了1.17亿户,相当于互联网2005年的网民人数,增长率已经连续两年超过100%。随着中国移动、中国电信和中国联通分别推出了3G上网方案,移动

互联网驶入了发展的快车道^[1-6]。

与此同时,移动互联网上的安全问题也逐渐显现出来。网络上出现了大量如:GTP over Billing攻击、DDoS攻击、DHCP地址耗尽攻击、伪冒地址恶意阻断上下文攻击、“沉默诅咒”拒绝服务攻击、垃圾信息群发、隐私信息窃取、手机病毒等在内的威胁互联网安全的案例。截至2008年底,能运行在智能手机平台上的病毒已经接近400个。移动互联网继承了传统互联网技术以及移动通信网技术的脆弱性,面临来自“问题多多”的互联网和正在IP化的移动网的双重安全风险威胁。可以预计,移动互联网安全问题将在不久的将来凸现出来,成为安全重灾区。

1 移动互联网

移动互联网的概念是相对传统互联网而言,强调可以在随时随地,

并且可以在移动中接入互联网并使用业务。与此类似还有无线互联网的概念,强调以无线方式而非同轴、双绞线、光纤等有线方式接入互联网并使用互联网业务。一般来说移动互联网与无线互联网并不完全等同:移动互联网强调使用蜂窝移动通信网接入互联网,因此常常特指手机终端采用移动通信网(如2G、3G、E3G)接入互联网并使用互联网业务;而无线互联网强调接入互联网的方式是无线接入,除了蜂窝网外还包括各种无线接入技术,例如便携式计算机采用802.11(Wi-Fi)技术接入互联网并使用互联网业务。

随着电信网络和计算机网络在技术、业务方面的相互融合:手机除了通过移动通信网外也可以通Wi-Fi接入互联网;便携式计算机除了通过无线局域网(如Wi-Fi)外也可以使用数据卡通过移动通信网接入互联网。很多人已经不再纠缠移动互联网与无线互联网的细微差别。一般人们可以认为移动互联网是采用手机、个人数字助理(PDA)、便携式计算机、专用移动互联网终端等作为终端,移动通信网络(包括2G、3G、E3G等)或无线局域网作为接入手段,直接或通过无线应用协议(WAP)访问互联网并使用互联网业务。移动互联网网络结构如图1所示。

与此对应,移动互联网安全研究采用手机、PDA、便携式计算机、专用

基金项目: 国家高技术研究发展计划(“863”计划)资助项目(2008AA01A204)

28

中兴通讯技术

2009年8月 第15卷第4期 Aug. 2009 Vol.15 No.4

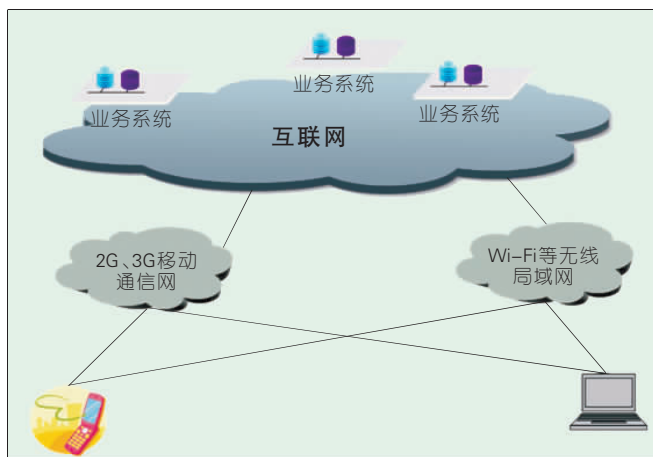


图1
移动互联网网络结构

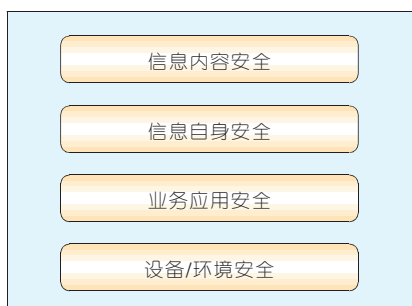


图2 网络与信息安全分层

移动互联网终端等作为终端,移动通信网络(包括2G、3G、E3G等)或无线局域网作为接入手段,直接或通过WAP访问互联网并使用互联网业务时的安全问题。

2 移动互联网安全架构

2.1 网络与信息安全分层

移动互联网既涉及传统的移动通信网络(现包含电路域和分组域),又涉及被公认安全问题比较严重的互联网,相关网络与信息安全研究相对复杂,应当分层研究。通常基础网络安全研究可以分4层研究,如图2所示。

(1)设备/环境安全

设备/环境物理安全通常是指网络、主机、终端等设备所处环境温度、湿度、电磁、防尘、防火、门禁、访问控制等条件符合必要的标准要求;操作系统、数据库、中间件、基础协议栈等具备必要的防攻击、防入侵能力;保

障设备稳定可靠稳定运行。

(2)业务应用安全

对于通信网络而言,业务一般是指和网络捆绑紧密,由网络向用户提供的服务;应用是指在网络之上,将网络作为通道为用户提供的服务。业务应用安全通常是指业务应用正常提供、用户可靠接入、计费管理等信息安全、信令等控制信息安全,防止非授权使用、服务滥用、服务盗用、DDoS攻击、服务否认、信令干扰等。

(3)信息自身安全

信息自身安全包括信息完整性、机密性和不可否认性:信息完整性可以依靠报文鉴别机制例如哈希算法等来保障;信息机密性可以依靠加密机制以及密钥分发等来保障;信息不可否认性可以依靠数字签名等技术保障。

(4)信息内容安全

信息内容安全通常是指传播信息不包含违反国家相关法律法规明文禁止发布和传播的违法信息;违背社会主义精神文明建设要求、违背中

华民族优秀传统文化与习惯以及其他违背社会公德的不良信息;侵犯公民隐私的个人敏感信息;垃圾信息、病毒等。

2.2 移动互联网安全

依据无线互联网网络架构网络与信息安全分层,移动互联网安全可以分为互联网终端安全、移动互联网网络安全以及移动互联网业务安全3个部分分别研究,如图3所示。

2.2.1 移动互联网终端安全

移动互联网终端通常是指手机、PDA、上网本、便携式计算机等。移动互联网终端安全可以按照网络与信息安全,分设备/环境安全、业务应用安全、信息自身安全以及信息内容安全4个层面进行研究。

(1)设备/环境安全

手机等移动互联网终端属于信息技术设备和电信终端设备,首先应符合包括电磁兼容(EMC)和电器安全在内的中国强制认证(CCC)要求;其次移动互联网终端使用无线电技术,应符合无线电管理局(SRRC)的型号核准认证(TYC);第三手机等电信终端设备应符合包括网络安全要求在内的工信部的通信入网认证(NAL)。此外移动互联网终端多属智能设备,通常具备操作系统,应当对常见的病毒、如木马、钓鱼和针对操作系统、应用程序漏洞的攻击具备一定的防范能力。

(2)业务应用安全

移动互联网终端的业务应用安全通常用于终端配合网络设备,确保

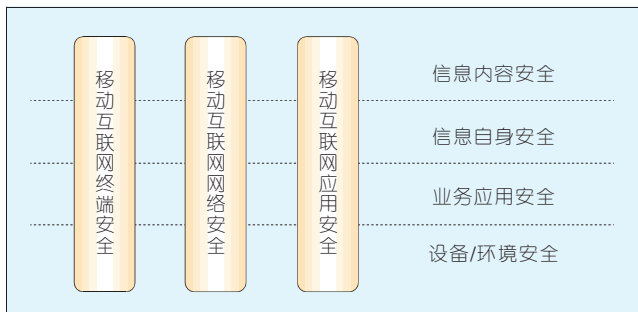


图3
移动互联网安全架构

合法用户可以正常使用,防止业务被盗用、冒名使用等,防止包括用户密码在内的用户隐私信息泄露,在承诺范围内随时使用,防范DDoS等攻击,必要的加密、隔离等手段保障通信秘密等。使用移动通信网作为接入手段时,终端相关的接入安全在设备/环境安全(电信终端设备入网要求)和移动互联网网络安全中考虑。因此业务应用安全主要考虑与接入无关的应用安全。

(3)信息自身安全

移动互联网终端的信息自身安全主要是指存储在终端中(包括通信录、通话记录、收发的短信/彩信、IMEI号、SIM卡内信息、用户文档、图片、照片在内)的用户隐私信息、个人信息不被非法获取。用户信息在传递中的保密性、完整性和可用性在互联网网络安全以及业务应用安全中考虑。终端的信息自身安全主要考虑终端内信息的授权访问、防入侵、加密存储等。

(4)信息内容安全

移动互联网终端信息内容安全涉及较少,当前主要关注保护青少年在使用移动互联网的过程中免受包括黄色、淫秽、暴力在内的不良信息侵扰。

2.2.2 移动互联网网络安全

移动互联网网络分两部分,接入网以及IP承载网/互联网。接入网采用移动通信网时涉及基站(BTS)、基站控制器(BSC)、无线网络控制器(RNC)、移动交换中心(MSC)、媒体网关(MGW)、服务通用分组无线业务支持节点(SCSN)、网关通用分组无线业务支持节点(GGSN)等设备以及相关链路,采用Wi-Fi时涉及接入(AP)设备。IP承载网/互联网主要涉及路由器、交换机、接入服务器等设备以及相关链路。移动互联网网络安全同样分设备/环境安全、业务应用安全、信息自身安全以及信息内容安全4个层面进行研究。

(1)设备/环境安全

移动互联网设备/环境安全主要是指路由器等网络设备自身的安全性、所处环境符合标准要求等。上述设备自身安全主要包括符合工信部设备入网要求中的安全要求,环境安全主要是指上述设备所处环境温度、湿度、电磁、防尘、防火、门禁、访问控制等条件符合必要的标准要求。此外设备/环境安全还包括网络设备的操作系统、数据库、中间件、基础协议栈等具备必要的防攻击、防入侵能力;保障设备稳定可靠稳定运行。

(2)业务应用安全

移动互联网网络的业务应用安全主要是指接入服务的安全性,主要采用认证等技术手段确保合法用户可以正常使用,防止业务被盗用、冒名使用等。在2G的GSM网络中实施单向认证,采用A3/A8实现认证和密钥协商。在3G网络中以3GPP为例,在R99中引入了双向认证、新的鉴权算法:高级加密标准(ASE),将加密算法后移至无线网络控制器(RNC),引入新的密码算法Kasumi,增加了信令完整性保护;在R4中增加了MAPSec保护移动应用协议(MAP)信令安全;在R5中利用IPSec保护分组域安全,并引入IP多媒体子系统(IMS)接入安全;在R6中增加了通用鉴权架构。采用Wi-Fi接入时,有802.11i以及中国自主知识产权的无线局域网认证和保密基础设施(WAPI)提供接入安全。

(3)信息自身安全

移动互联网信息自身安全主要包括信息空口传播、IP承载网/互联网传递时网络所提供必要的隔离和保密以及接入网络所涉及的用户注册信息安全。虽然移动通信网中定义了空口加密算法,但是中国无论是2G网络还是正在部署的3G网络都没有实施。多数Wi-Fi的接入网也没有实施加密。因此信息自身安全主要依赖端到端实施。

(4)信息内容安全

移动互联网有大量业务来自传

统互联网,所传递的信息内容属于公众信息而不是端到端通信,因此移动互联网网络的内容安全应当涉及必要的有害信息过滤与检查。

2.2.3 移动互联网应用安全

移动互联网业务可以分为3类:第一类是传统互联网业务在移动互联网上的复制;第二类是移动通信业务在移动互联网上的移植;第三类是移动通信网与互联网相互结合,适配移动互联网终端的创新业务。当前可以预期的移动互联网业务包括利用智能手机等移动互联网终端获取的移动浏览、移动Web2.0、移动搜索、移动电子邮件、移动即时消息、移动电子商务、移动在线游戏、电话、短信、彩铃、彩信、移动定位、移动导航、移动支付、移动VoIP、移动地图、移动音频、移动视频、移动广告、移动Mashup、移动SaaS等。移动互联网应用安全也可以分设备/环境安全、业务应用安全、信息自身安全以及信息内容安全4个层面进行研究。

(1)设备/环境安全

移动互联网应用安全相关设备/环境安全主要是指应用服务器、Web服务器、数据库服务器、邮件服务器、网关、存储介质等设备自身的安全性、所处环境符合标准要求等。上述设备自身安全主要符合涉及电器安全的中国强制认证(CCC)认证要求,环境安全主要是指上述设备所处环境温度、湿度、电磁、防尘、防火、门禁、访问控制等条件符合必要的标准要求。此外设备/环境安全还包括上述的操作系统、数据库、中间件、基础协议栈等具备必要的防攻击、防入侵能力;保障设备稳定可靠稳定运行。

(2)业务应用安全

移动互联网业务应用安全主要是指业务应用的安全性,主要采用认证等技术手段确保合法用户可以正常使用,防止业务被盗用、冒名使用等。当前多数应用安全机制与网络层接入的安全机制无关,由移动互联网

终端与移动互联网业务设备端到端实施。

(3)信息自身安全

移动互联网应用安全中信息自身安全主要包括业务应用相关信息完整性、机密性和不可否认性。虽然网络可能采取一定的加密、隔离措施保障信息自身安全,但是当前移动互联网应用主要依靠移动互联网终端与移动互联网业务设备端到端实施。

(4)信息内容安全

移动互联网业务可以来自互联网、移动网以及移动网与互联网结合所得的创新业务。包括动浏览、移动Web2.0、移动搜索、移动地图、移动音频、移动视频、移动广告、移动Mashup在内的多数业务相关的信息属于公众信息而不是端到端通信。因此移动互联网应用应当采取足够有效的措施来防范应用所涉及内容不包括违法信息、不良信息以及侵犯公民隐私的敏感信息等。

3 移动互联网安全展望

移动互联网是一个新生事物。是移动通信网与互联网相结合的产物,既有来自互联网的基因也有来自移动网的基因,具备明显的杂交优势。

随着3G的部署、智能手机以及上网本的成熟,现已显示出勃勃生机。然而移动互联网相关的安全问题也逐渐显露出来,有来自互联网的病毒、垃圾信息等,也有来自移动网互联网相结合后的非法定位、移动网身份窃取等。随着3G网络的进一步建设、智能终端的普及以及对互联网需求以及依赖性的进一步增强,移动互联网用户规模和网络规模都将呈现爆炸性增长,移动互联网安全问题也即将随之凸显。

当前无论是移动互联网还是移动互联网的安全,与传统的互联网、互联网安全相比有较大的差距。其原因主要来源移动互联网终端带宽有限,计算能力有限,显示屏幕有限,内容源有限以及输入手段受限等。随着技术的发展与进步,移动互联网与传统互联网将逐渐趋同,用户将不再刻意区分是移动互联网还是传统互联网,使用有线上网还是移动网上网。但是在当前移动互联网发展初期,完全有机会依据移动互联网安全框架,通盘考虑安全需求与技术,使移动互联网乃至未来整个互联网都变得更安全。可以预期,移动互联网安全研究将在很长一段时间成为安全研究

的重点和热点。

4 参考文献

- [1] Mobile working needs a security rethink [EB/OL]. 2009-04-07. <http://www.zdnetasia.com/insight/security/0,39044829,62052863,00.htm>.
- [2] 陈灿峰. 宽带移动互联网 [M]. 北京: 北京邮电大学出版社, 2005.
- [3] 张惠媛. 移动互联网与WAP技术 [M]. 北京: 电子工业出版社, 2003.
- [4] Mobiles to come under attack from 'bad guys' [EB/OL]. 2008-04-25. <http://www.zdnetasia.com/news/communications/0,39044192,62040620,00.htm>.
- [5] Mobile security technology fights fraud [EB/OL]. 2008-06-20. <http://www.zdnetasia.com/news/security/0,39044215,62042941,00.htm>.
- [6] Botnets on cell phones in 2009? [EB/OL]. 2008-10-17. http://news.cnet.com/8301-1009_3-10067994-83.html.

收稿日期: 2009-05-11

作者简介



魏亮, 信息产业部电信传输研究所副总工程师兼网络与信息安全中心主任, 主要从事网络架构、下一代互联网、网络与信息安全等领域的研究工作。现为ITU-T SG17 Q8报告人。已主持/参加3项国家高技术研究发展计划(“863”计划)项目。已发表学术论文8篇。

中兴通讯与印尼最大运营商Telkomsel签订GSM/UMTS建设合同

【本刊讯】2009年6月24日, 中兴通讯与印尼第一大运营商Telkomsel签署了GSM/UMTS建设合同。自2008年底中兴通讯先后获得香港CSL和中国联通UMTS建设项目以来, 目前在国际上已先后获得土耳其第三大运营商AVEA、越南第一大运营商Viettel、印尼第一大运营商Telkomsel的多个重要合同。上述国家均为人口排名全球前20的大国。

合同的签署标志着中兴通讯正式成为Telkomsel在GSM/UMTS领域的战略合作伙伴, 成为短名单内的主要供应商。按照合同约定, 中兴通讯将为Telkomsel建设领先的GSM/UMTS网络。

中兴通讯执行副总裁田文果说, “作为在亚太地区有着很强影响力的运营商, Telkomsel选择中兴通讯一定能带动双方在未来的双赢。中兴通讯的创新科技和定制化的无线产品解决方案一定能帮助Telkomsel巩固其在印尼和整个亚洲市场的领先地位”。

Telkomsel总裁Mr Sarwoto在致辞中表示, “很高兴中兴通讯成为Telkomsel的战略合作伙伴。Telkomsel致力于提供优质网络给印尼的终端客户, 相信中兴通讯业界领先的GSM/UMTS解决方案、优异的产品性能和出色的售后能力将帮助Telkomsel巩固在业界的领先地位。同时, Telkomsel将在2010年新增加147个城市的3G网络部署并开通高速数据业务, 和中兴通讯的强强联合一定能使双方获益”。